From Bridges and Rockets, Lessons for Software Systems

C. Michael Holloway

17th International System Safety Conference
August 1999
Orlando, Florida

Outline

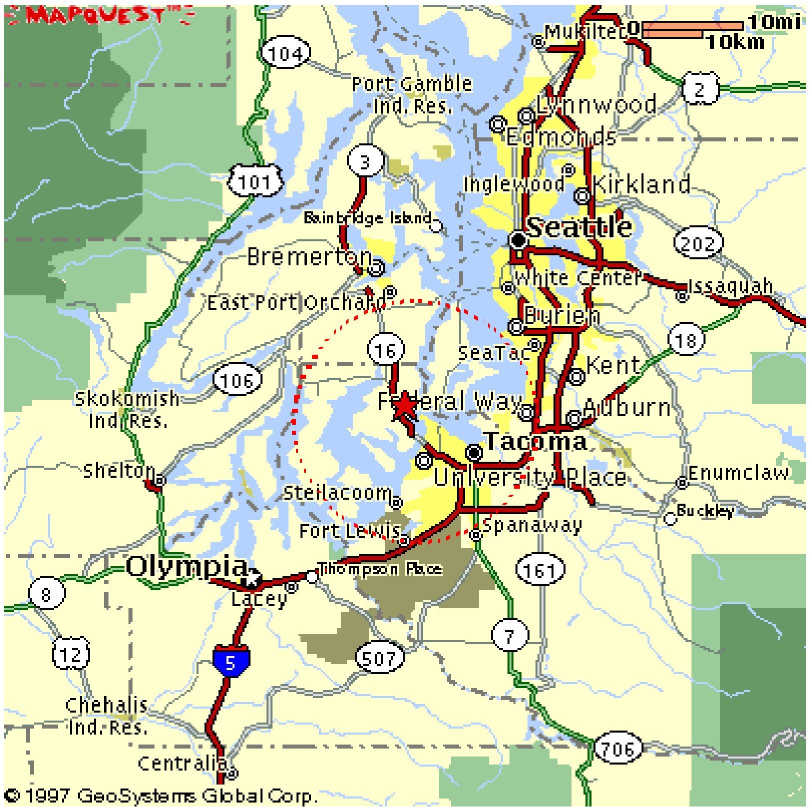
- Motivation for the paper
- Brief summaries of the accidents
  - Tacoma Narrows Bridge
  - Space Shuttle Challenger
- Five lessons taught by these accidents
- Three applications of these lessons to software systems
- Concluding remarks

Motivation

- General
  - Weary with “software is <u>so</u> different” claims
  - Henry Petroski, *To Engineer is Human: The Role of Failure in Successful Design*
  - Desire to establish foundation for rationale for research about accident analysis
- Specific
  - Henry Petroski, *Engineers of Dreams: Great Bridge Builders and the Spanning of America*
  - Diane Vaughan, *The Challenger Launch Decision*

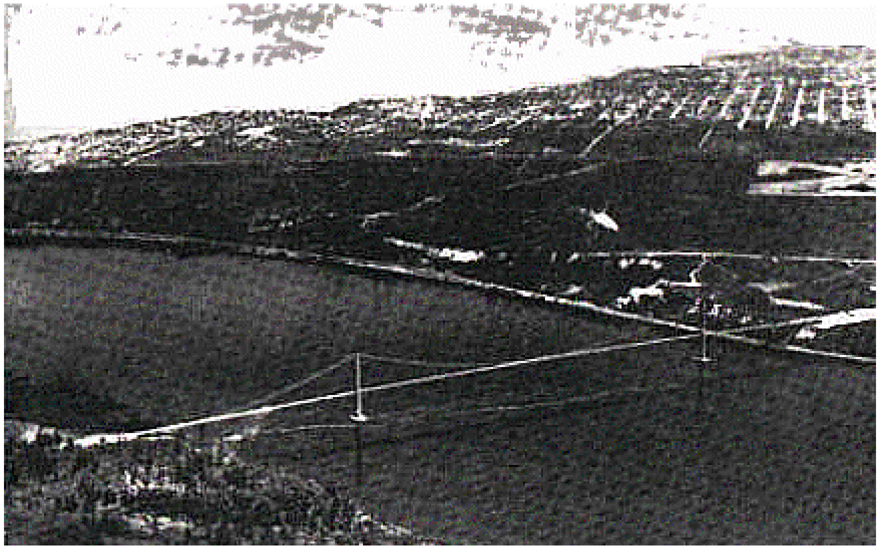
Tacoma Narrows Bridge

Location & Basic Facts



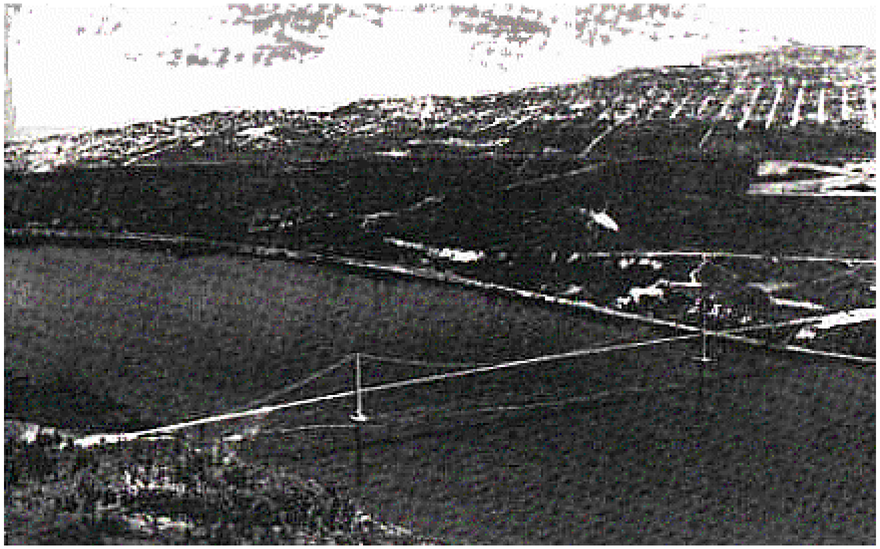
Tacoma Narrows Bridge

Location & Basic Facts



Tacoma Narrows Bridge

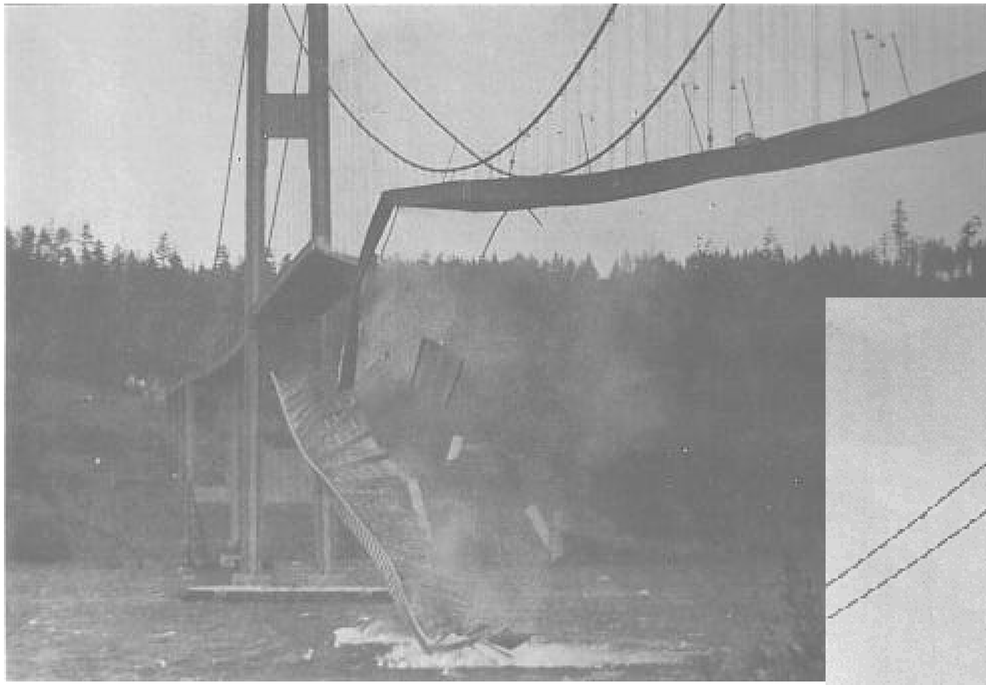
Location & Basic Facts

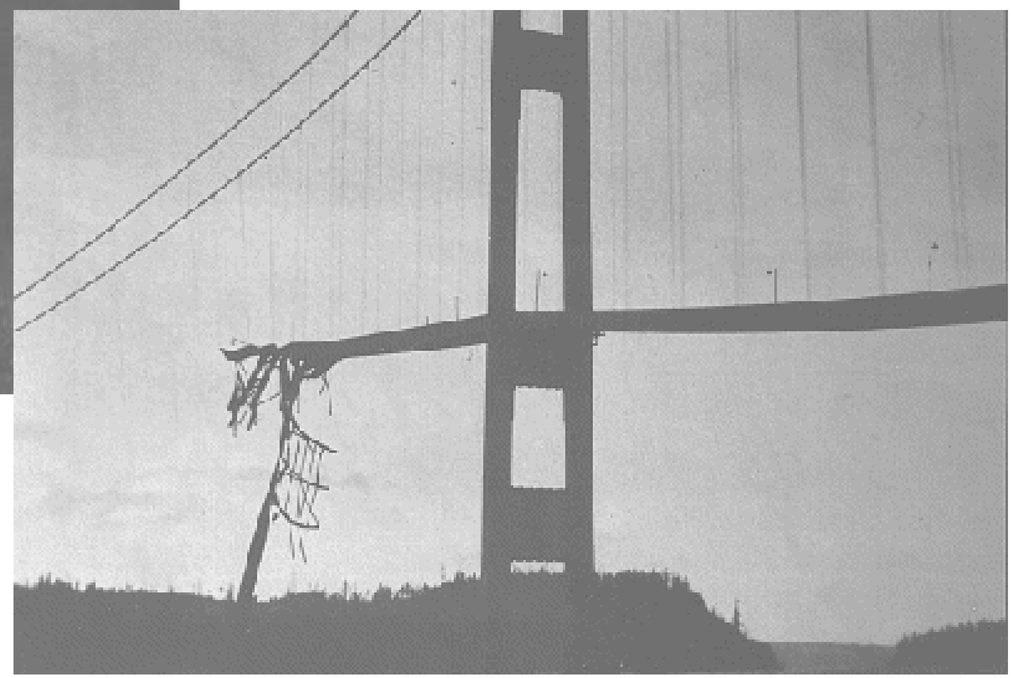


- Completed in 1940
  - 2800' main span — 3rd longest
  - Designed by Leon Moisseiff
- Very narrow and shallow
  - 39' wide
  - 8' deep plate girders
- Extremely flexible in the wind
  - Noticed during construction
  - Nicknamed "Galloping Gertie"

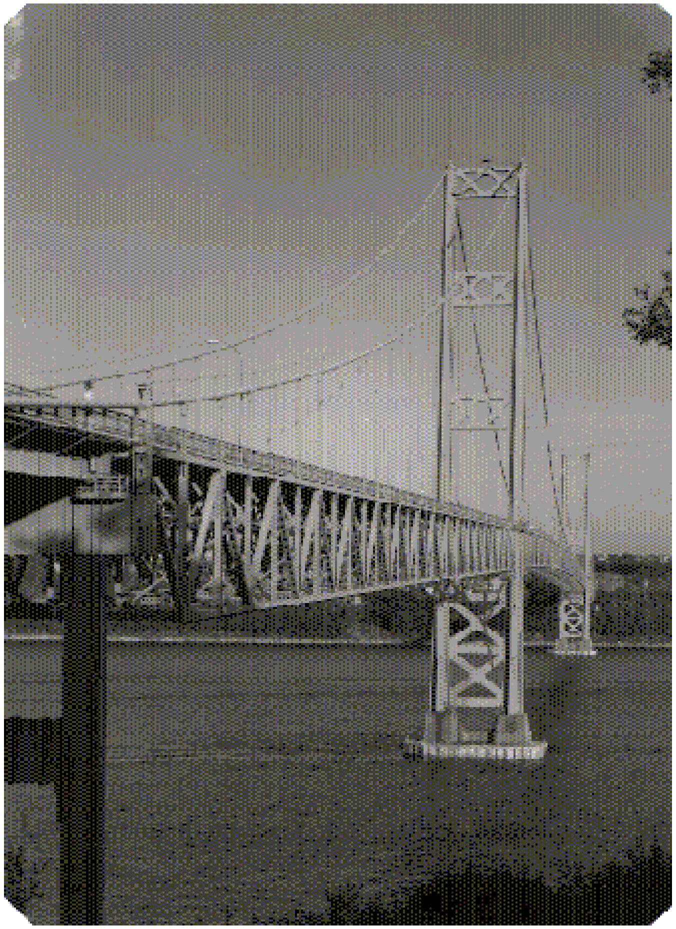
Bridge Collapse Movie

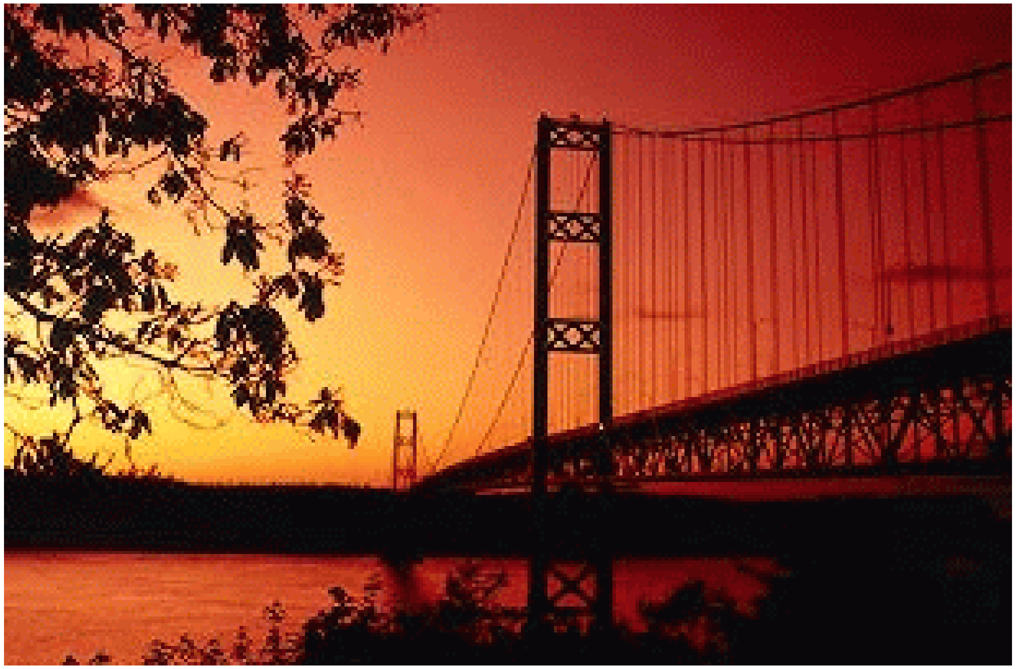
Bridge Collapse Photographs





Current Tacoma Narrows Bridge





Challenger Accident

Background

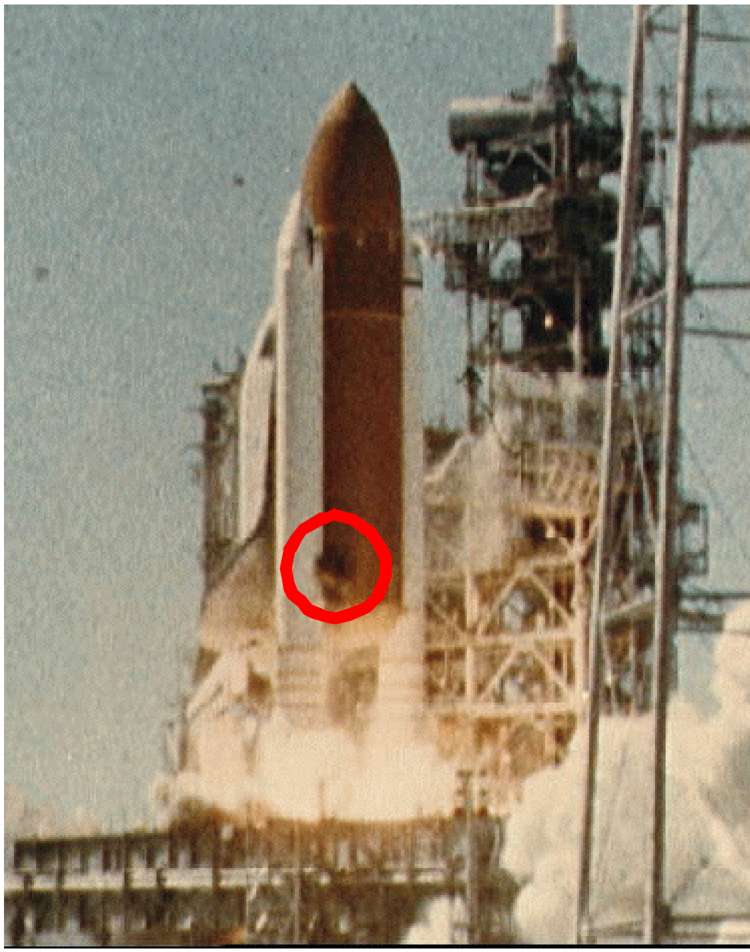
- Mission 51-L launched on January 28, 1986
  - Several delays
  - Tenth launch for Challenger
- Several objectives
  - deploying a Tracking and Data Relay Satellite
  - deploying the Spartan-Halley satellite
- Included “teacher-in-space”

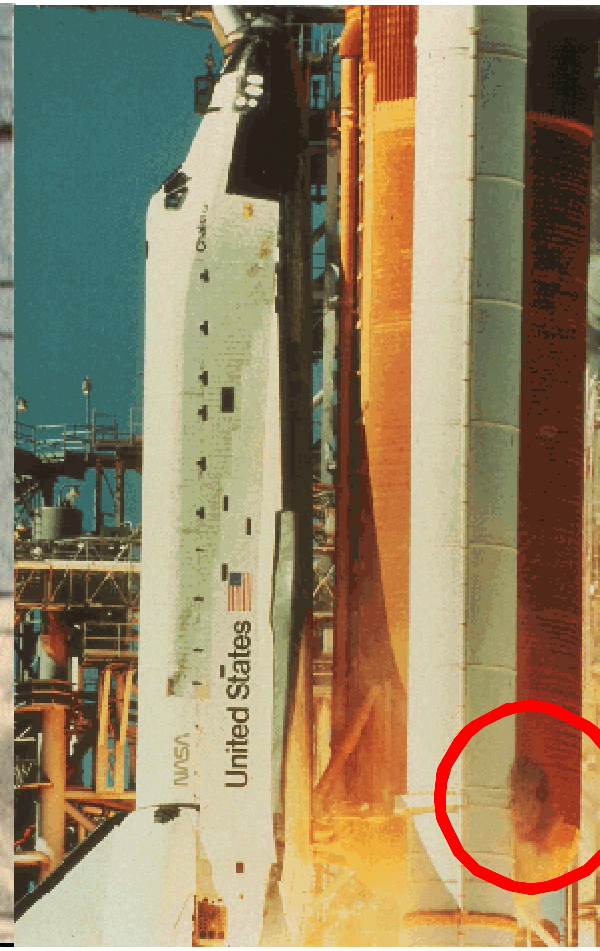
Challenger Accident

From afar, the launch looks normal ...

Challenger Accident

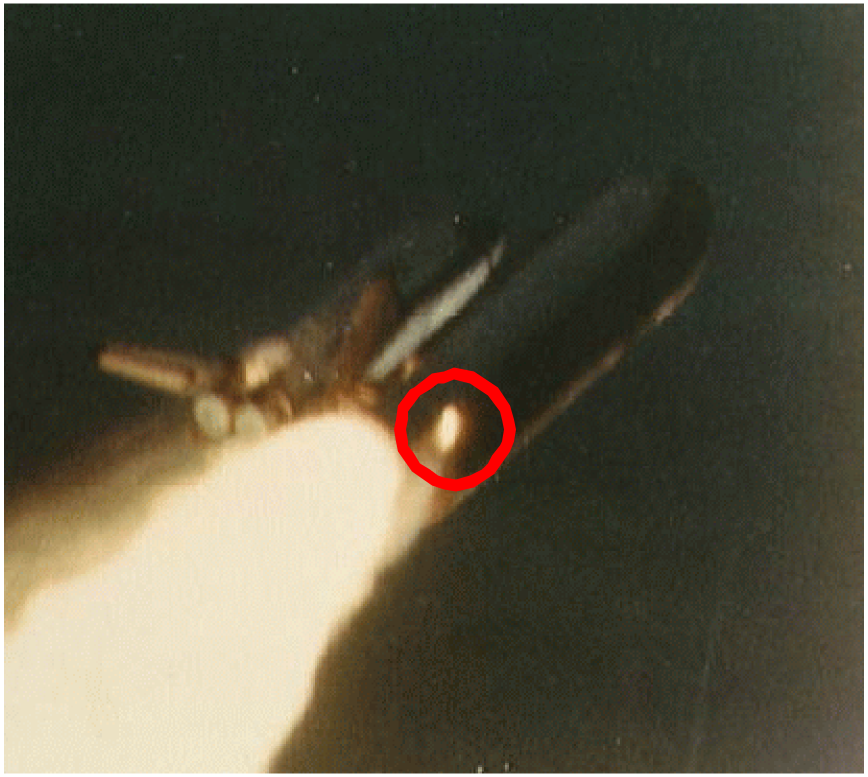
... but it isn't

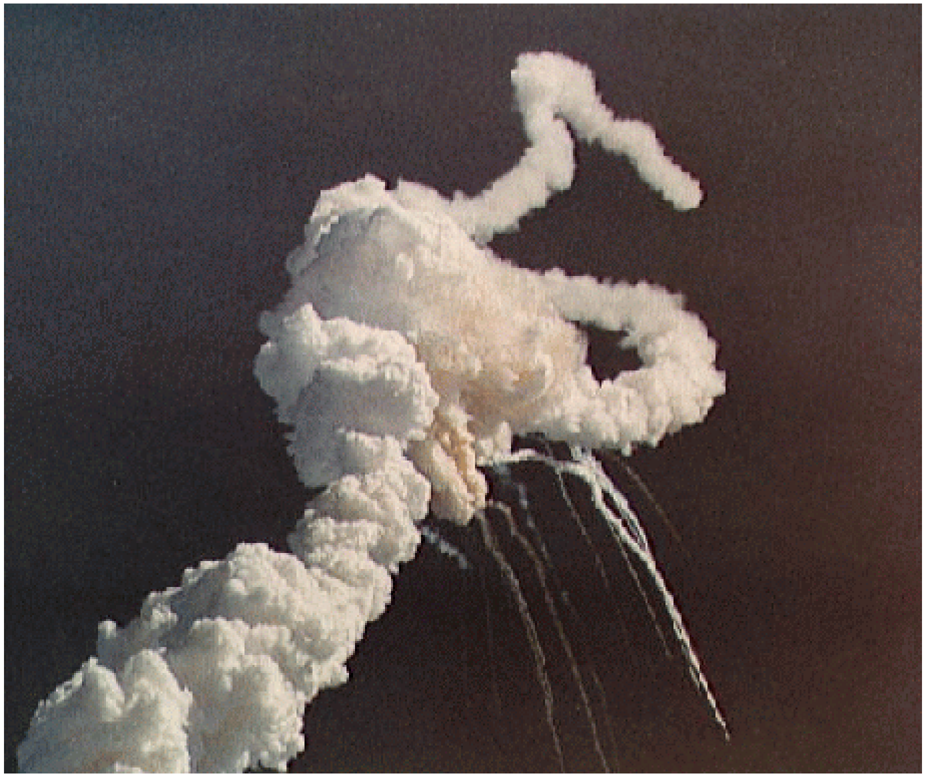




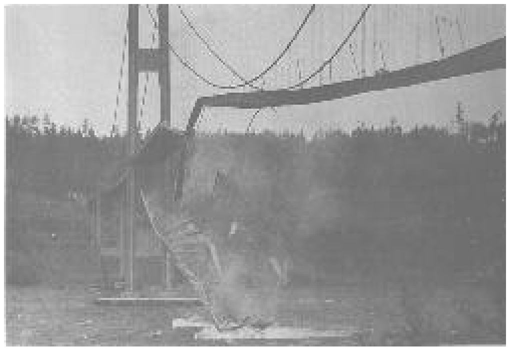
Challenger Accident

Final failure





Lessons Taught



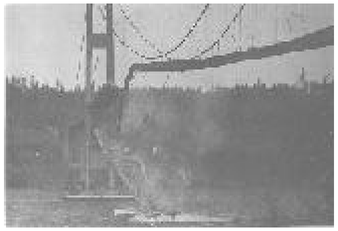
Relying heavily on theory, without adequate confirming data, is unwise

Relying heavily on data, without an adequate explanatory theory, is unwise

Going well beyond existing experience is unwise

In studying existing experience, more than just the recent past should be included

When safety is concerned, misgivings on the part of competent engineers should be given strong consideration, even if the engineers can not fully substantiate these misgivings

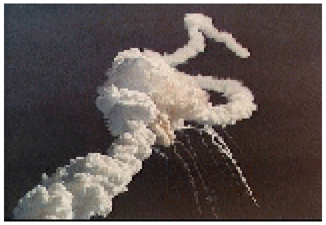


Relying heavily on theory, without adequate confirming data, is unwise

Don’t Rely on Theory Alone

- Narrowness and shallowness of bridge was based on deflection theory
  - Scale model experiments had agreed with theory’s predictions for lateral deflections
  - No experimental data on vertical deflections
  - Theory partially used for some existing bridges
- The first real test of the theory was above the waters of the Puget Sound
  - Other bridges showed less severe problems
  - These problems were corrected by various means

Don't Rely on Data Alone



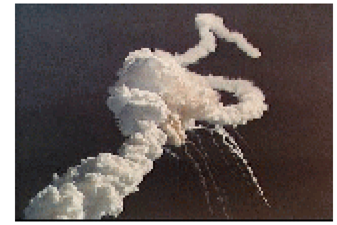
Relying heavily on data, without an adequate explanatory theory, is unwise

- As early as 1977, tests of the solid rocket motor failed to confirm design assumptions
  - Assumption was that propellent pressure at ignition would cause the inner flanges of the tang and clevis of a joint to bend **towards** each other, ensuring that O-rings would seal the joint
  - The opposite actually happened: immediately after ignition, the tang and clevis moved **away** from each other, thus reducing compression on the O-rings

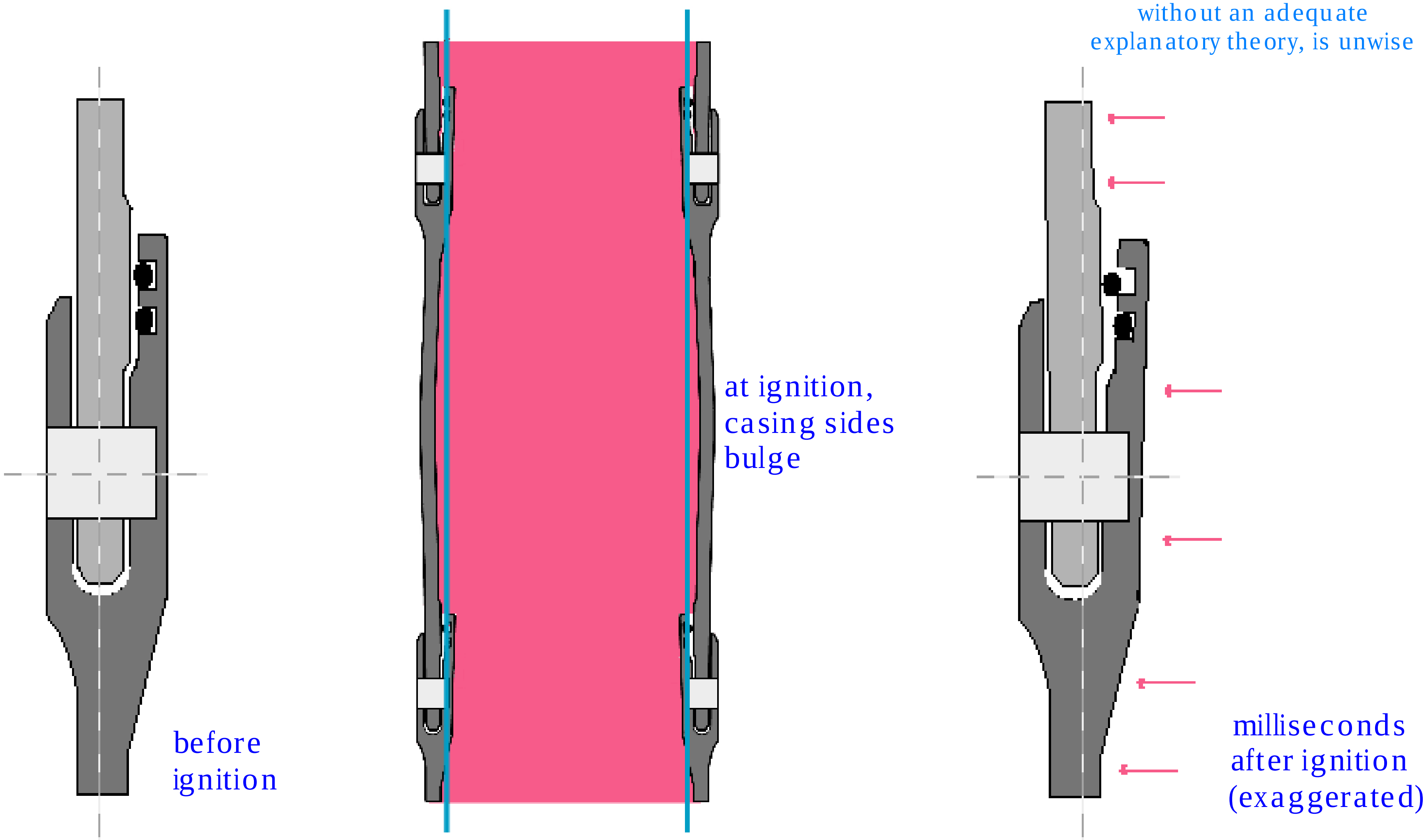
Joint Rotation

Don’t Rely on Data Alone

Continued

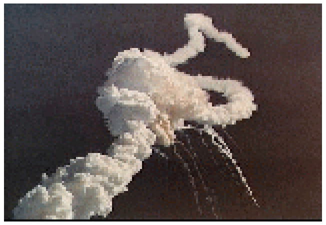


Relying heavily on data, without an adequate explanatory theory, is unwise



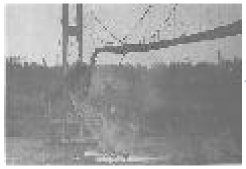
Don't Rely on Data Alone

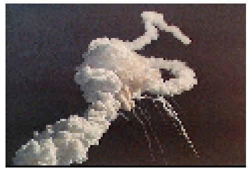
Continued 2



Relying heavily on data, without an adequate explanatory theory, is unwise

- At the time of Challenger's last flight, no theory fully explaining joint rotation had been developed
- The rationale for the safety of the joints was based on extrapolations from tests and flights
  - At least one O-ring always sealed
  - This "confirmed" the belief that the maximum possible gap size was small enough to not be a danger to the safety of flights

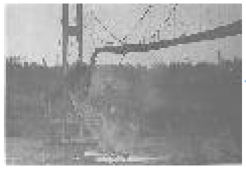


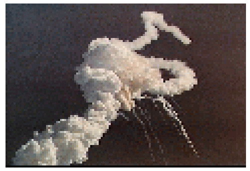


Respect Experience

- Although the Tacoma Narrows Bridge was not the longest suspension bridge, it had a span to width ratio significantly larger than any other existing bridge

Bridge	Span:Width Ratio
Delaware River	1:19.7
Whitestone	1:31
San Francisco Bay	1:35
George Washington	1:33
Golden Gate	1:46.7
Tacoma Narrows	***1:72***



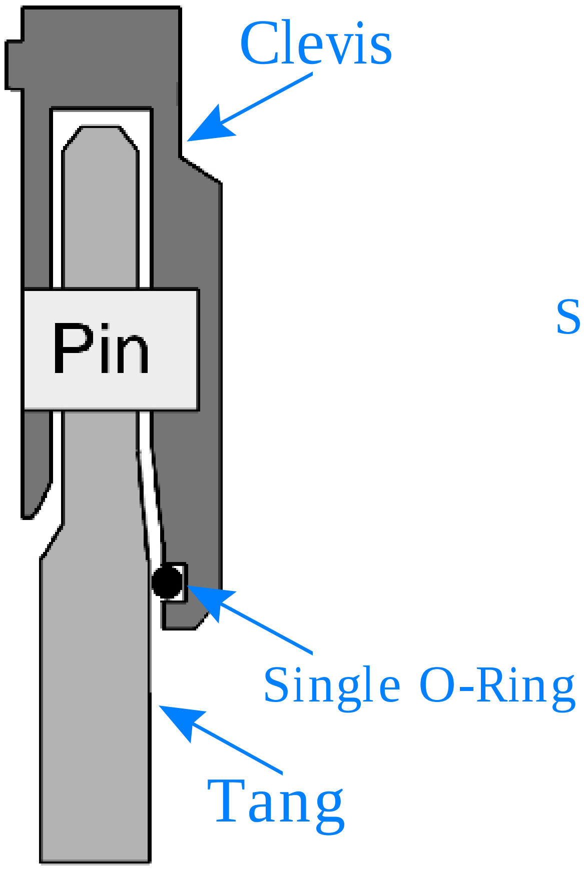


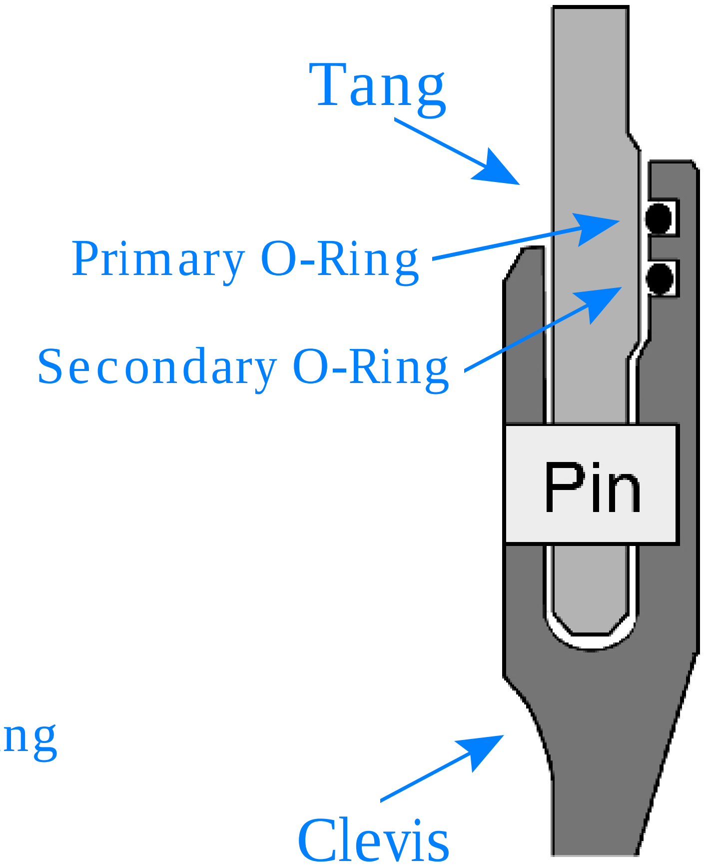
Respect Experience

Continued

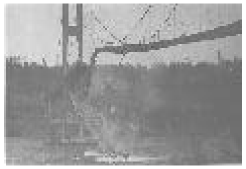
Going well beyond existing experience is unwise

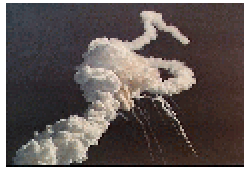
Titan III Joint





SRB Joint

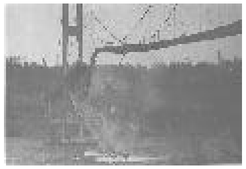


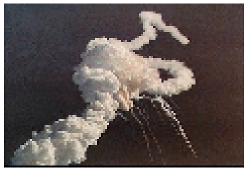


Study History

In studying existing experience, more than just the recent past should be included

- A 1949 report showed that suspension bridge failure under dynamic wind loads had been frequent in early to mid 1800's
  - Engineers had learned to prevent such failures by making the bridges sufficiently wide and stiff
  - This knowledge had been partially lost in the 1900's
- Some parallels seem to exist between attitudes in the shuttle program before Challenger and in the Apollo program before the 1967 fire

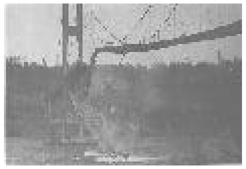


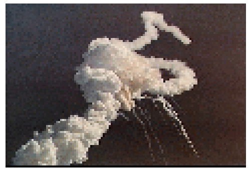


Listen to Warnings

When safety is concerned, misgivings on the part of competent engineers should be given strong consideration, even if the engineers can not fully substantiate these misgivings

- Advisory Engineer Theodore Condron warned about the possibility of failure of the bridge
  - He eventually acquiesced to the design, based primarily on Leon Moisseiff's stellar reputation
  - But he still suggested widening the bridge by 13'
- Events before the Challenger accident are well-known
  - Some Morton-Thiokol engineers objected to launching until the temperature got warmer





Listen to Warnings

When safety is concerned, misgivings on the part of competent engineers should be given strong consideration, even if the engineers can not fully substantiate these misgivings

A Caveat

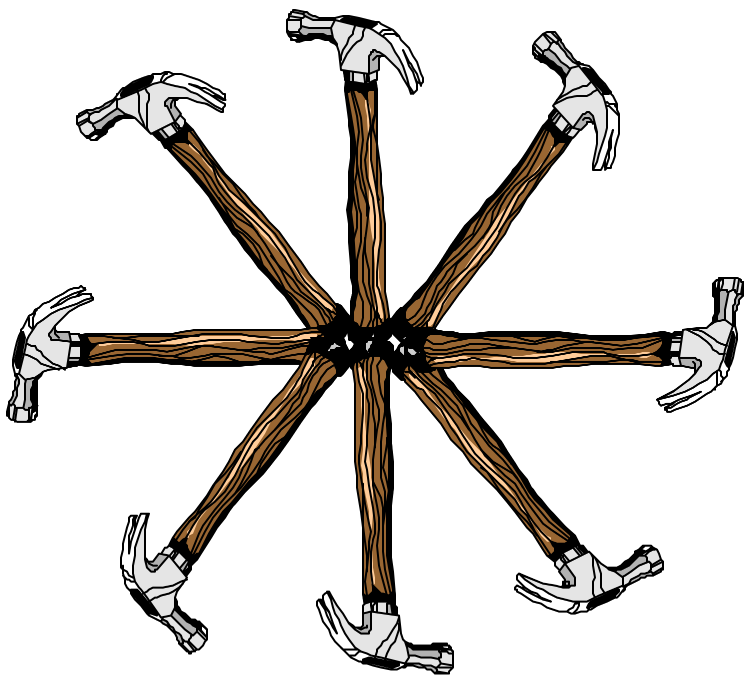
First Application to Software

Relying heavily on theory, without adequate confirming data, is unwise

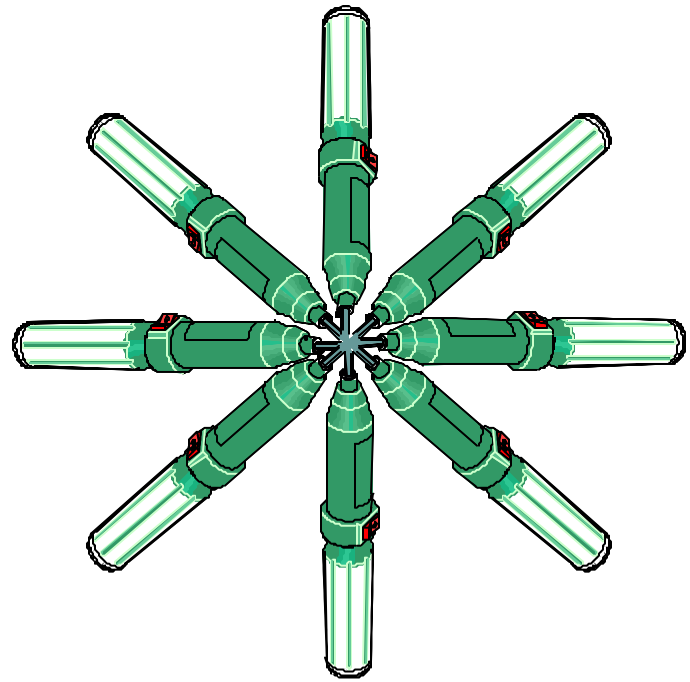
Relying heavily on data, without an adequate explanatory theory is unwise

The verification and validation of a software system should not be based on a single method, or a single style of methods

Which is a Better Set of Tools?

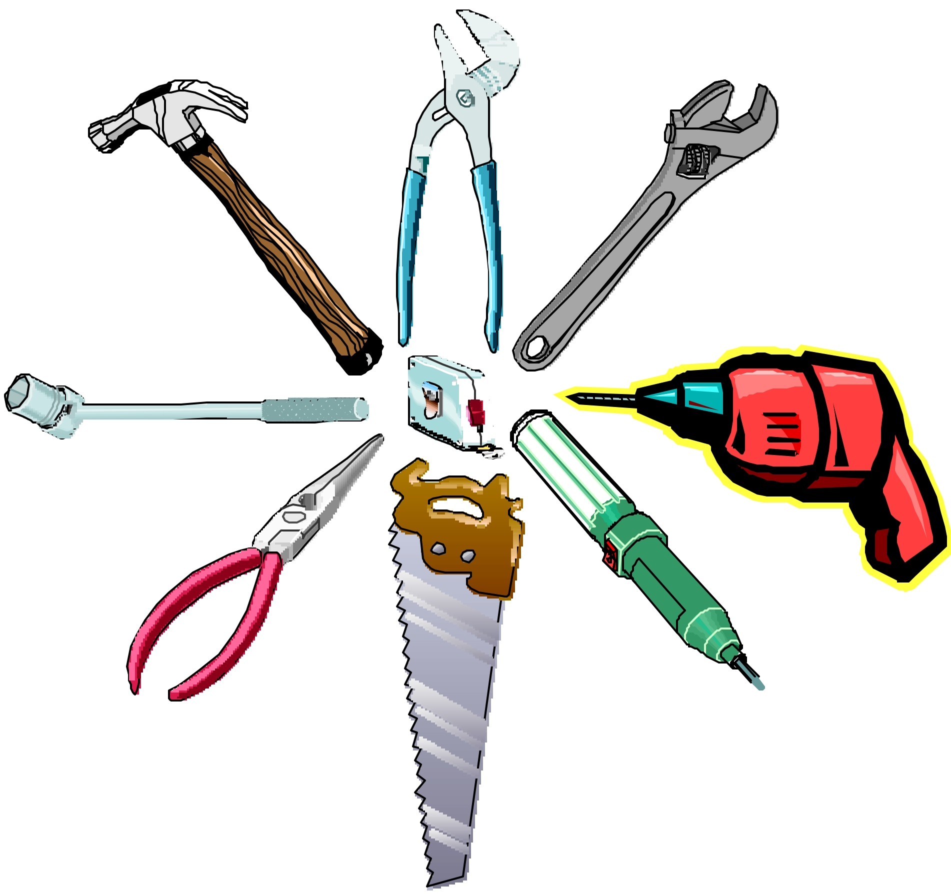


or



It is a meaningless question:
Neither one is sufficient by itself!

We Need Many Different Tools



- Getting these tools requires cooperation, not competition
- Formalists and testers need to be friends, instead of foes

Second Application to Software

In studying existing experience, more than just the recent past should be included

The tendency to embrace the latest fad must be overcome

Fad-ism Prevails

- The history of software development seems to be characterized by one fad after another
  - Someone comes up with a good idea
  - People learn about the idea and begin applying it to everything
  - Zealots proclaim that the solution to the "software crisis" is at hand
- Current fads: object-orientation, process improvement
- Future fads: soft computing, virtual reality

Defeating Fad-ism

- Recognize that it exists
- Study original sources, not derivatives
  - Originators rarely make the outlandish claims that later supporters do
  - Learn the limitations
- Read Fred Brooks' 1987 article, "No Silver Bullet: Essence and Accidents of Software Engineering", at least once a month

Third Application to Software

Going well beyond existing experience is unwise

... misgivings on the part of competent engineers should be given strong consideration ...

The introduction of software control into safety-critical systems should be done cautiously

Use Software with Caution

- The very "softness" of software makes the temptation great to try to use it for most everything
- Use should be guided by successful past experiences, not by ambitious future dreams
  - Too often software systems are conceived that bear no resemblance to what has been done before
  - Had NASA taken the same approach to the moon landing, "Apollo 11" would've been launched a few months after Friendship 7 splashed down

Concluding Remarks

- No software system failure so far has been analogous in its public impact to either the Tacoma Narrows Bridge collapse or the Challenger accident
- Understanding the fallibility of humans, and knowing a little bit about the history of technology, suggests that such catastrophes will happen
- If software engineers and managers are diligent to learn the lessons taught by the past, perhaps these catastrophes can be reduced in frequency and in severity